

DSI : une confiance aveugle dans les certificats TLS ?

Comment les directeurs des systèmes d'information (DSI) perçoivent le risque lié à la multiplication des identités de machines physiques (serveurs, PC, terminaux mobiles, objets connectés) et virtuelles (API, conteneurs...) à gérer ? C'est la question posée dans le cadre d'une [étude](#)* publiée par Venafi, fournisseur spécialisé de solutions.

79% des répondants disent connaître le nombre de clés et de certificats [TLS](#) (Transport Layer Security) utilisés par leur entreprise. 93% estiment à au moins 10 000 le nombre de certificats TLS sur lesquels s'appuie leur organisation pour protéger les identités machine. 97% des DSI prévoient une hausse de 10 à 20% du nombre de ces certificats TLS en 2021.

Selon l'étude, ces chiffres sont encore sous-estimés.

Certificats expirés

« De nombreux DSI sont susceptibles de largement sous-estimer le nombre d'identités machine TLS actuellement utilisées. Par conséquent, ils ne connaissent pas la taille de la surface d'attaque ni les risques opérationnels que ces identités machine inconnues font courir à leur société », a déclaré Kevin Bocek, VP stratégie de sécurité de Venafi.

Or, 75% des décideurs IT concernés se disent préoccupés par les risques de sécurité liés à la multiplication désordonnée des certificats TLS. Par ailleurs, une majorité (56%) déclare redouter les pannes et les interruptions potentielles d'activité liées aux certificats expirés.

De surcroît, des certificats contrefaits peuvent aussi être utilisés par des pirates informatiques pour intercepter des communications chiffrées entre clients et serveurs.

Pour le responsable stratégie de sécurité et renseignement sur les menaces de Venafi, « qu'il s'agisse de pannes associées à des certificats expirés ou d'attaquants qui se cachent dans un trafic chiffré pendant de longues périodes, les risques abondent. La seule façon d'y remédier consiste à détecter, surveiller et automatiser le cycle de vie de tous les certificats TLS sur l'ensemble du réseau de l'entreprise, y compris les certificats de courte durée utilisés dans les environnements cloud, virtuels et [DevOps](#). »

*Pour Venafi, Coleman Parkes a interrogé 550 DSI. France, Allemagne, Royaume-Uni, États-Unis et Australie sont couverts.

(crédit photo via pexels)